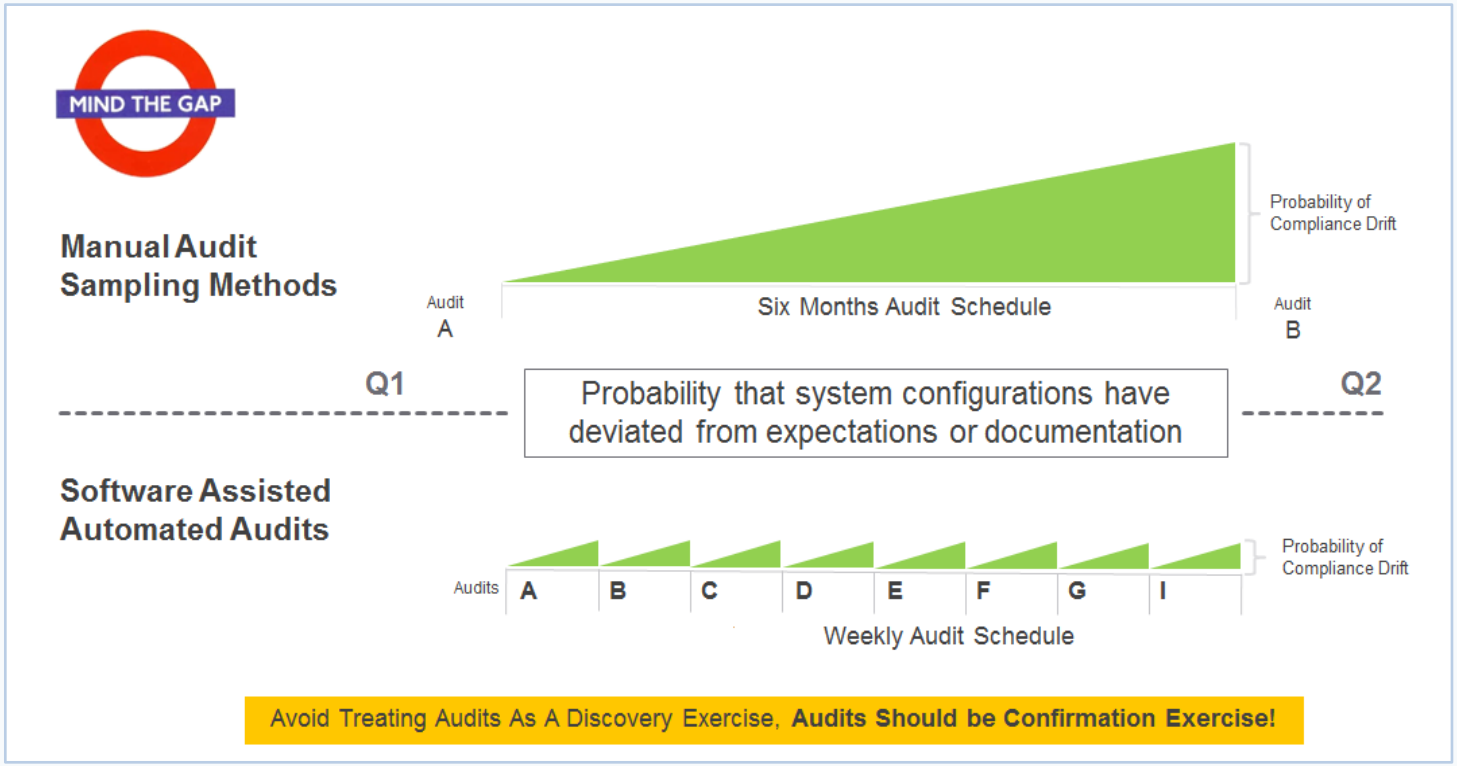
Continuous Compliance in Hybrid Environment

New Frontier in Unified Compliance, Configuration and File Integrity Management

Shailesh Athalye

VP, Compliance Solutions, Qualys, Inc.

2014: Good Old Days of Compliance

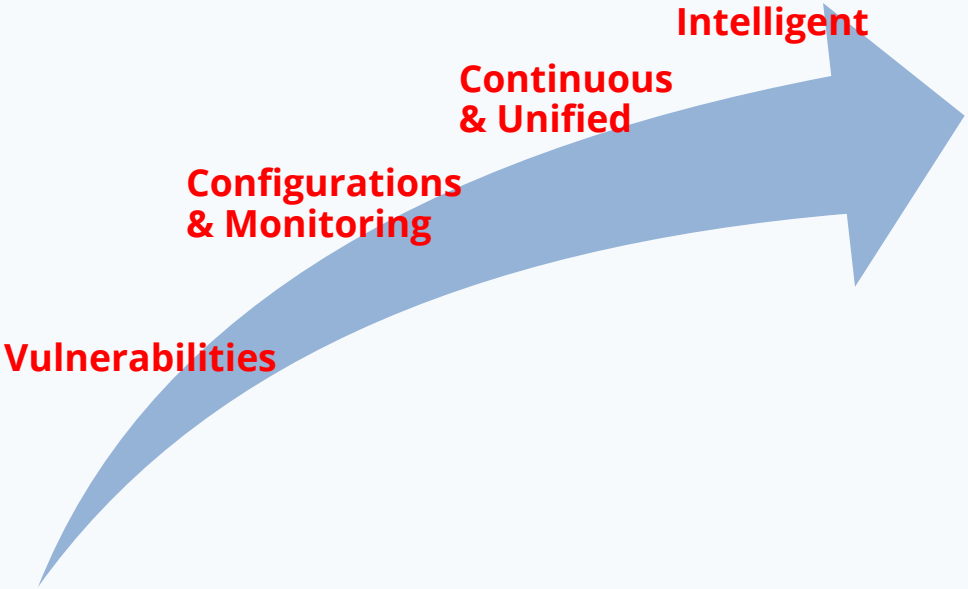


2020: Security is Continuous and Unified

To reduce the ‘attack surface’

To reduce breaches due to misconfigurations, lack of monitoring

Question remains:
How to make Compliance and Risk continuous?



Semi-automated Way for Connecting is old!

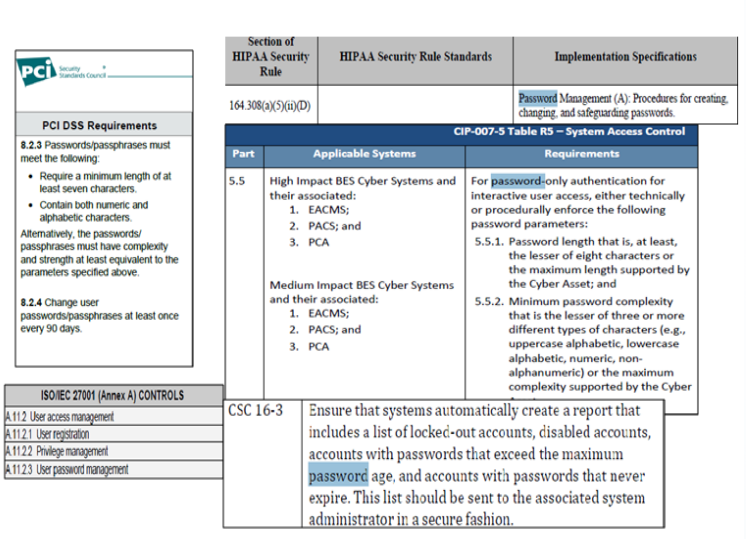
Time to value

Time to see roll up the operational data

Varied types of Security and Assets data
- FIM, Patch, Malware, VM, threats
- Scoping and Tracking Assets

Point solutions injecting data with connectors, never normalize

Connect Security with Compliance and Risk



PCI DSS Requirements

8.2.3 Passwords/passphrases must meet the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.2.4 Change user passwords/passphrases at least once every 90 days.

Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications
164.308(a)(5)(ii)(D)		Password Management (A): Procedures for creating, changing, and safeguarding passwords.

CIP-007-5 Table R5 – System Access Control

Part	Applicable Systems	Requirements
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber

ISO/IEC 27001 (Annex A) CONTROLS
A.11.2 User access management
A.11.2.1 User registration
A.11.2.2 Privilege management
A.11.2.3 User password management

CSC 16-3	Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.

Inventory Your Systems

Inventory and Restrict Software

Secure Configurations and Data Security

Continuous VM

Review Access Rights

AI SYN

SYN AI VM PC

PC

VM CM TP

PC

Continuous Compliance & Risk From Continuous Security

Qualys Unified Compliance & Risk

Map security to compliance

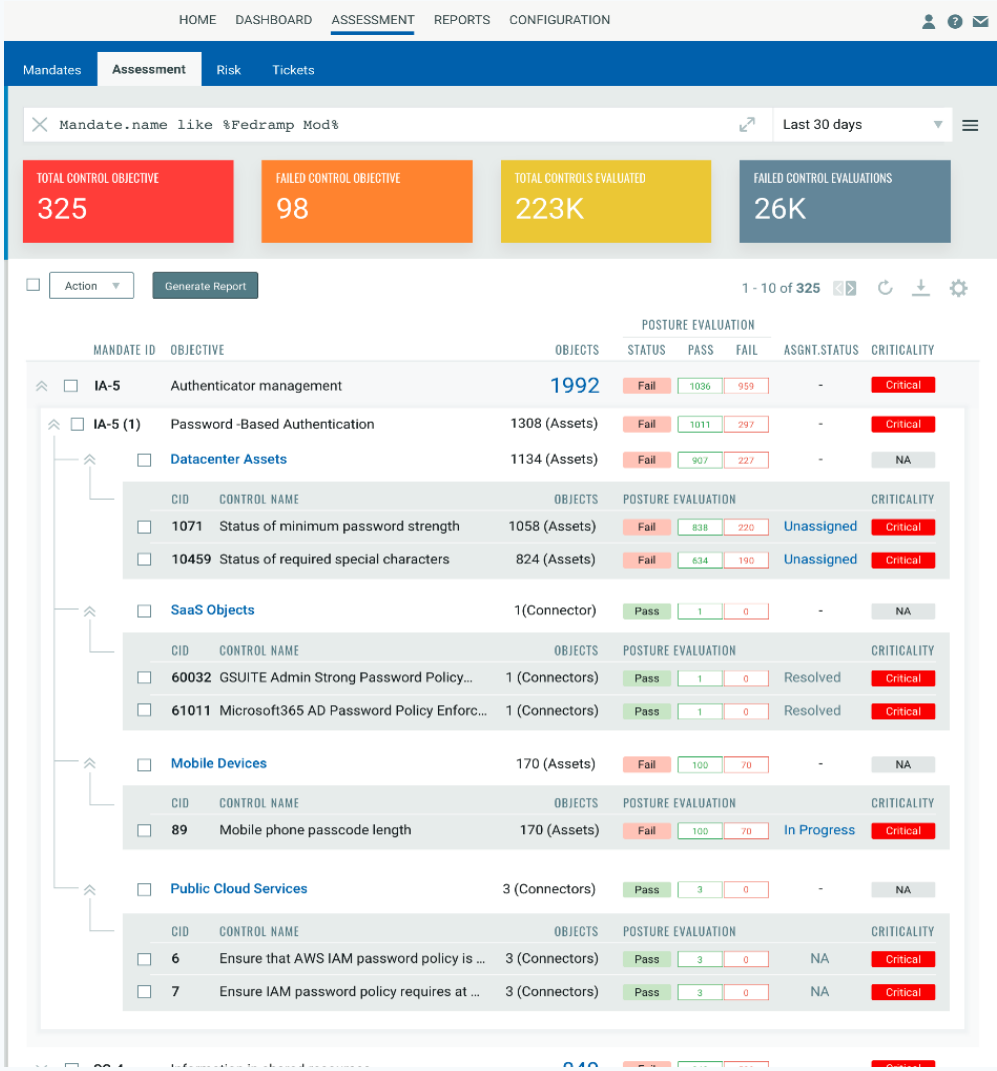
Integrated Security Platform

Qualys Platform for unified and continuous security

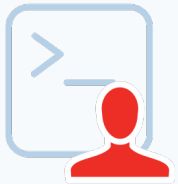
Qualys.

Continuous Risk and Compliance from Continuous Security

Qualys Unified Compliance maps every app's output to 25+ Compliance standards and Risk objectives

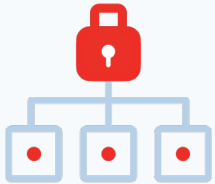


New-age Challenges: Teams Speaking Different Languages



Elastic, Kafka, custom web servers

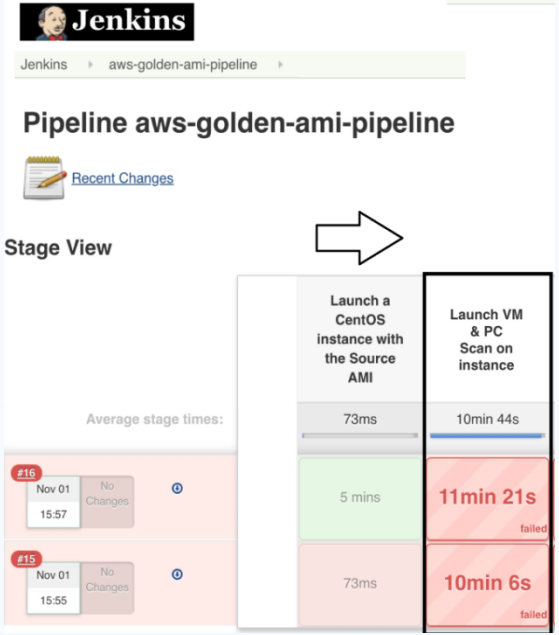
Identify risk and compliance



Secure hosts, config/integrity/ vulnerability management

Security & Compliance teams should be running with DevOps from the start

Start Compliant, Stay Compliant in DevOps with Qualys PC in CI Phase



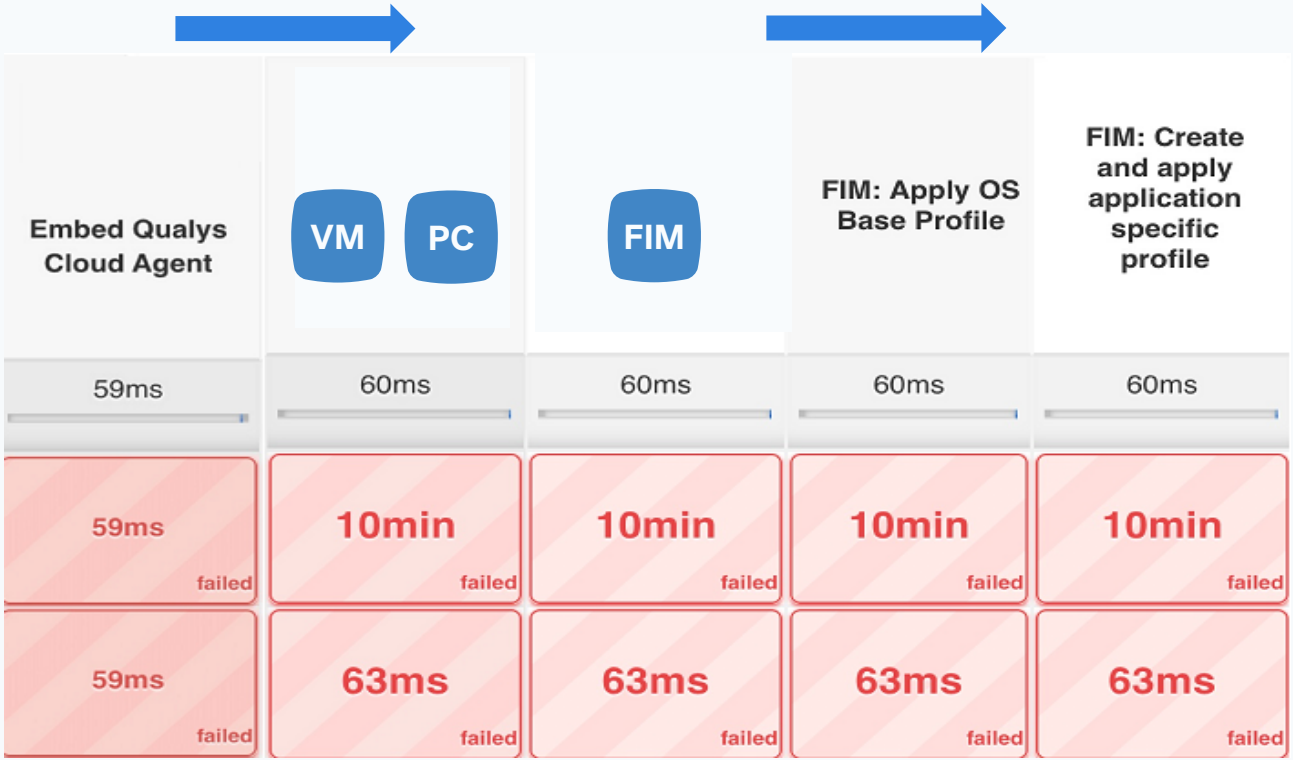
QUALYS POLICY COMPLIENCE RESULTS

Show 10 entries

CID	Title	Technology	Criticality
14602	Status of the 'nosuid' option for '/tmp' partition using 'mount' command	CentOS 7	4
10804	Status of the SELinux current mode (running configuration)	CentOS 7	4
10643	Status of iptables package	CentOS 7	4
12815	List of runtime audit rules for '/etc/passwd' file, using auditctl	CentOS 7	4
10664	Status of the 'OPTIONS' setting within '/etc/sysconfig/chronyd' file	CentOS 7	4
9473	Existence of the 'extraneous' files and directories (Sensitive files/Directories)	Tomcat 8	3
9477	Status of 'X-Powered-By' setting within 'server.xml' file	Tomcat 8	4
9551	Status of the 'secure' attribute for each 'Connector' elements whose 'SSL Enabled' are set to 'true'	Tomcat 8	4
9605	Status of the command-line flag 'STRICT_SERVLET_COMPLIANCE' set for the Tomcat process	CentOS 7	4
9565	Status of the 'web server processes' which are not started with 'Security Manager'	CentOS 7	4

Qualys.

Qualys FIM Monitors From CD Phase

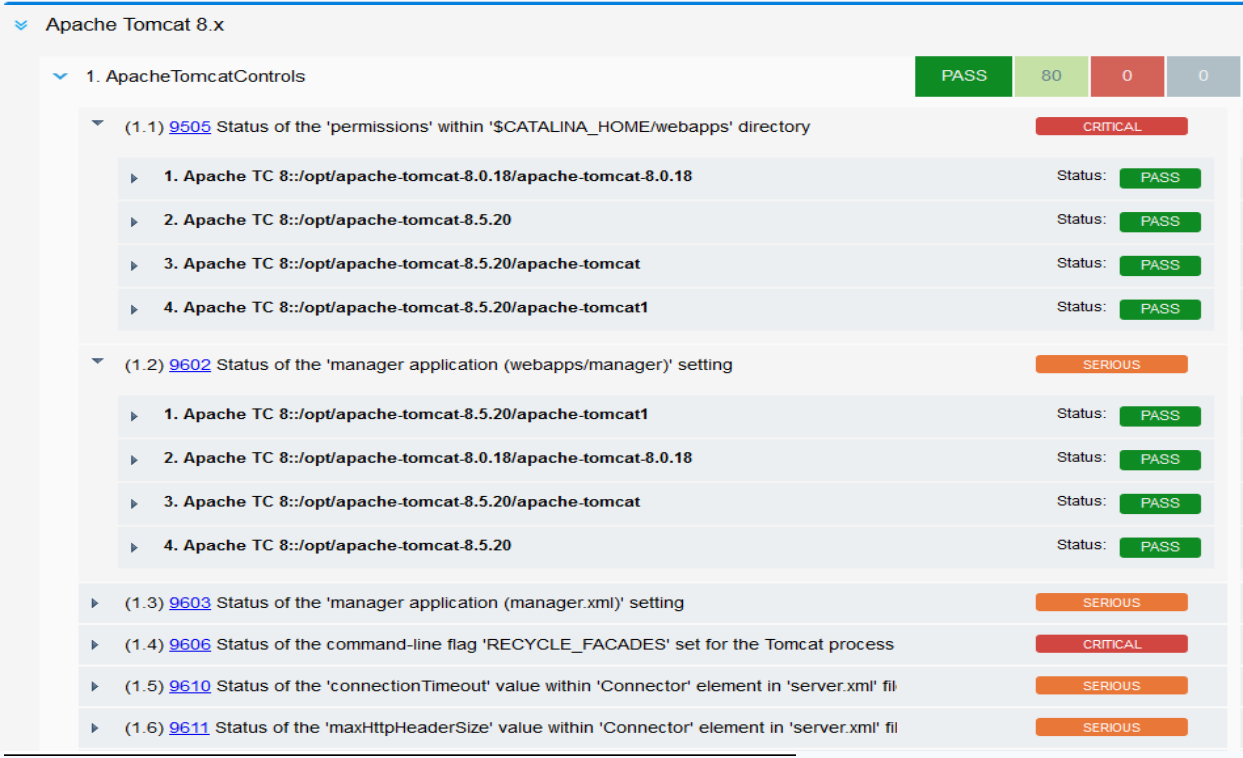


Qualys.

Automatically Discover and Assess Middleware with Dynamic Paths

Just based on host scans, discover unauthorized technologies, web servers, databases automatically

And…
There's no need to create authentication records



CISO Responsibility: Ensure Security Controls are in Place and Functioning

https://www.bitsight.com/blog/ciso-roles-and-responsibilities

Is Anti-virus active, updated for signatures, scanning?

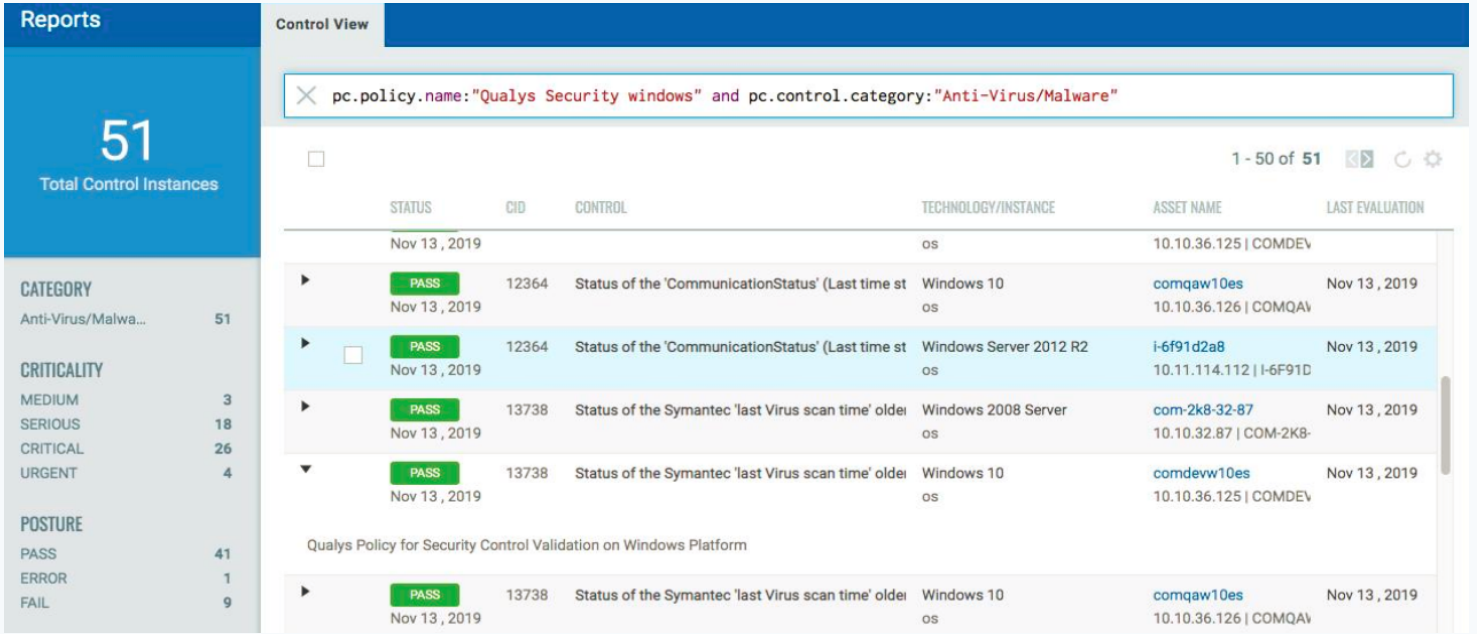
Is FIM, EDR agent configured correctly to monitor?

Are OS native application protection, memory protection configured?

Need to have Security Control Validation (SCV) in place to test and confirm that security tools have their pre-requisites in place and are configured properly on all endpoints

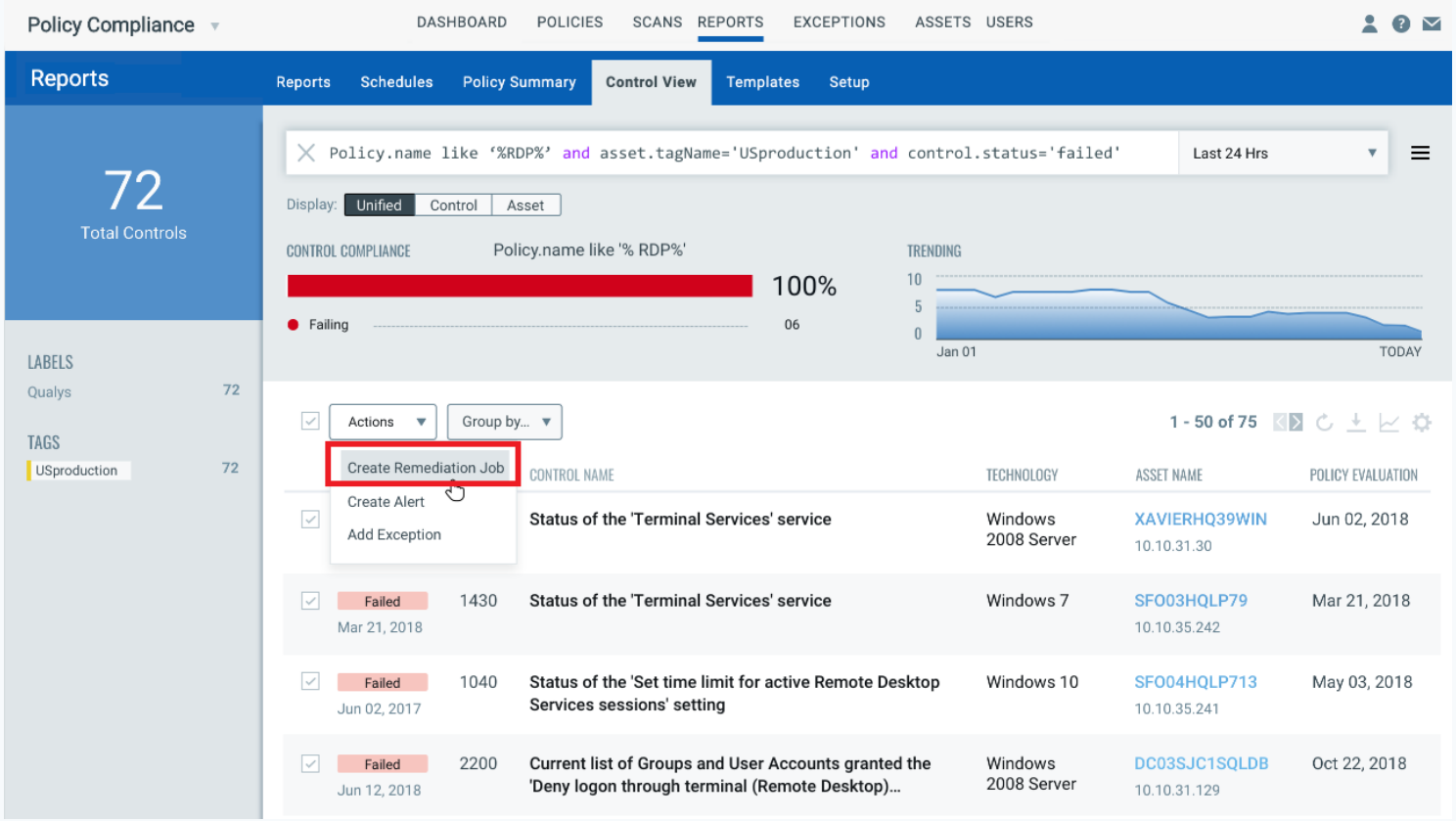
Security Control Validation from Policy Compliance

Anti-Virus technologies | Qualys FIM Agent | Splunk | Kafka | Native Malware Protection



Qualys.

Start Gold, Continuously Assess, Remediate



Qualys.

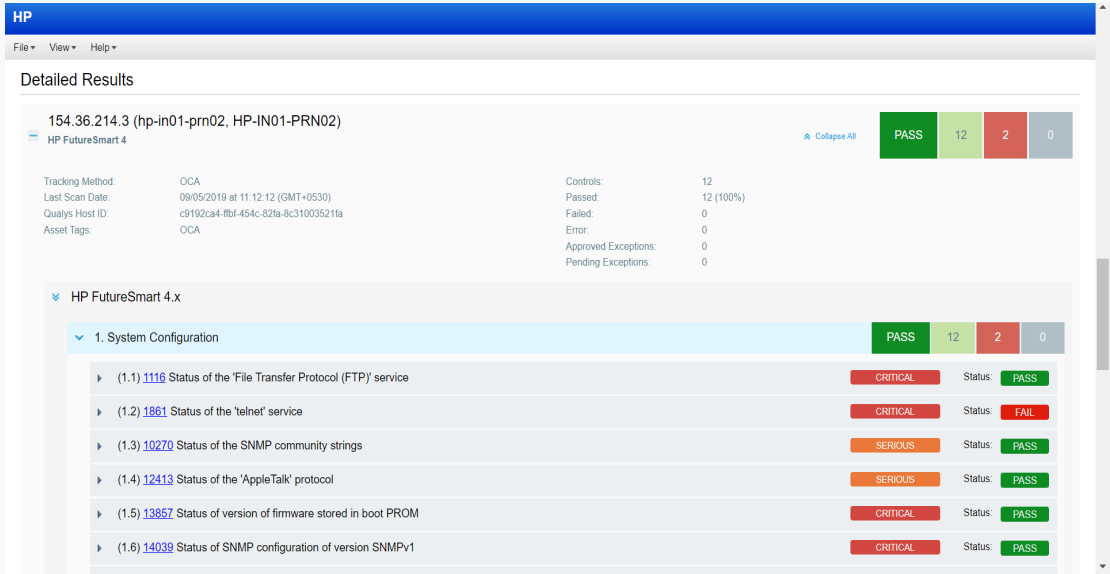
Network Devices, Printers and sensitive hosts can’t be Scanned but are in Security & Compliance Scope

Use Qualys Out-of-Band Config Assessment (OCA)

- Create custom assets
- Push command output, vulnerability, config data

Controls validate settings

Report vulnerabilities, security and misconfigurations



Policy Compliance

Best in class technology and content coverage For Configuration Management

>450 Policies, >14,000 controls
>150 technologies (traditional, emerging)
> Widest coverage for CIS, STIG, Mandates and beyond
> Qualys security experts author CIS benchmarks

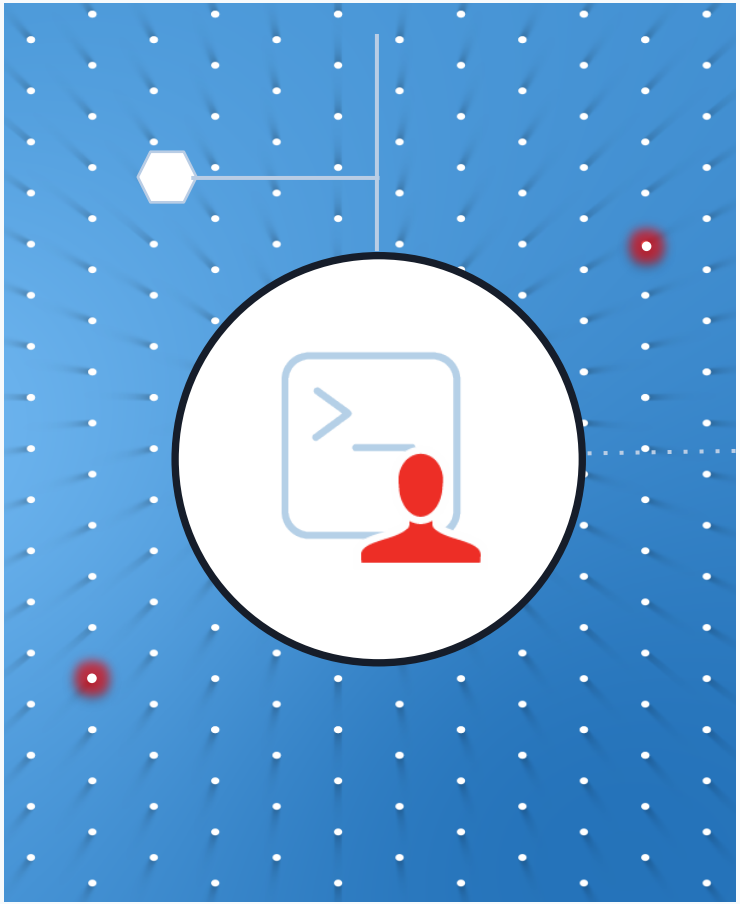
Data collection from all Qualys sensors

Custom database security & integrity controls

Auto-discovery of middleware technologies

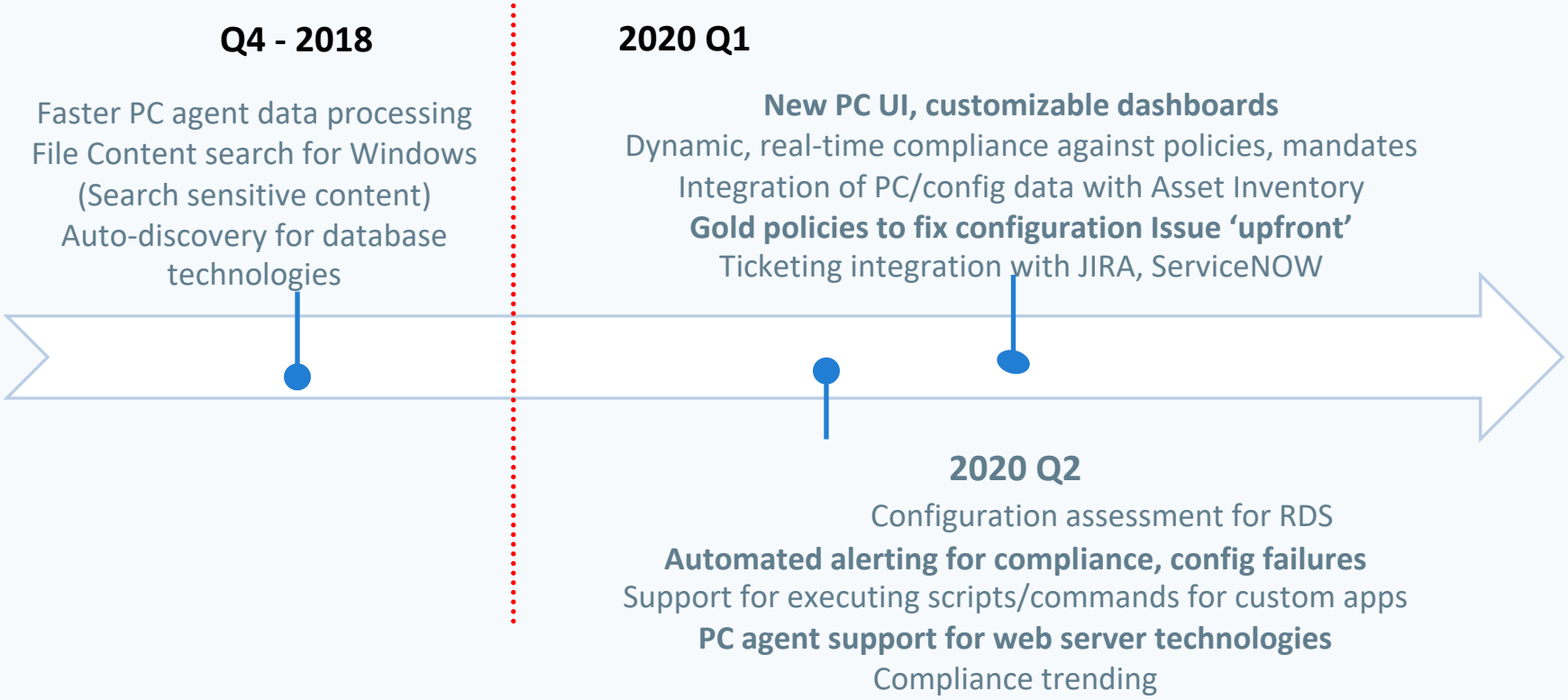
File, Directory Integrity, Network Shares Monitoring

Auto-remediation for configuration failures



New PC UI and Customizable Dashboard

Policy Compliance Roadmap

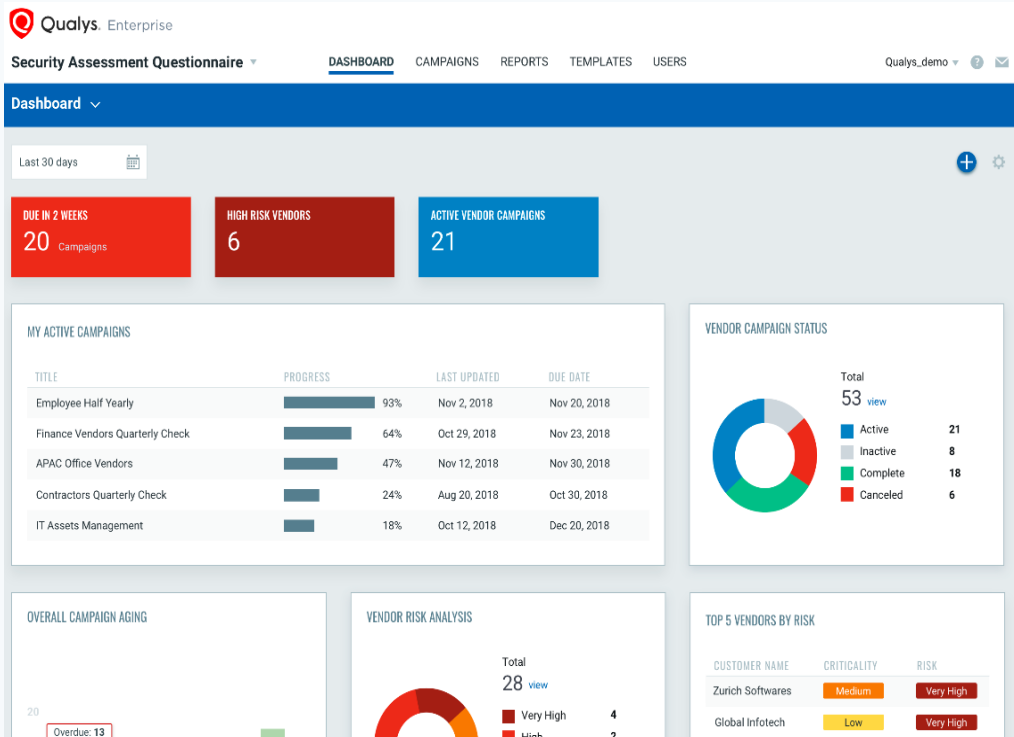


Qualys.

Your security is only as strong as your weakest vendor

Qualys Security Assessment Questionnaire (SAQ) helps in in managing vendor risk per vendor criticality

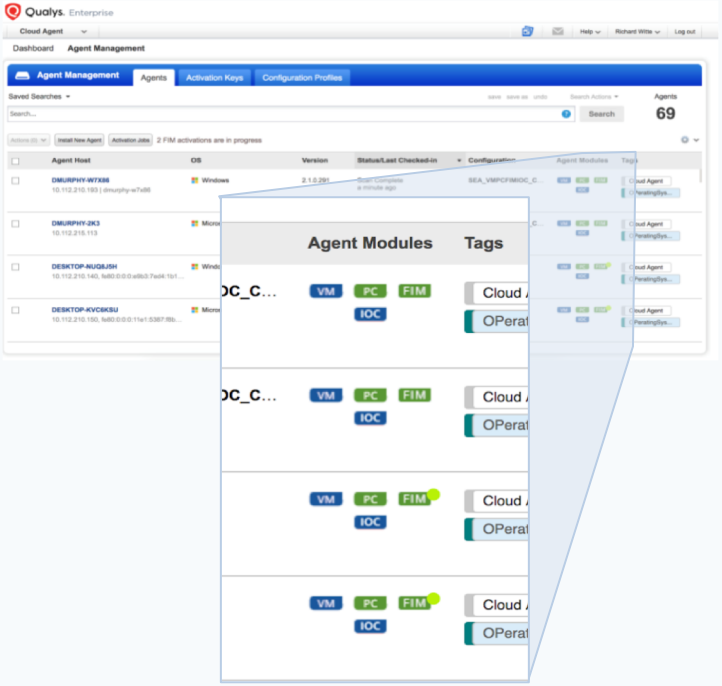
With **SAQ,** consolidate your vendor security and process compliance with technical security posture on the same platform



File Integrity Monitoring (FIM)

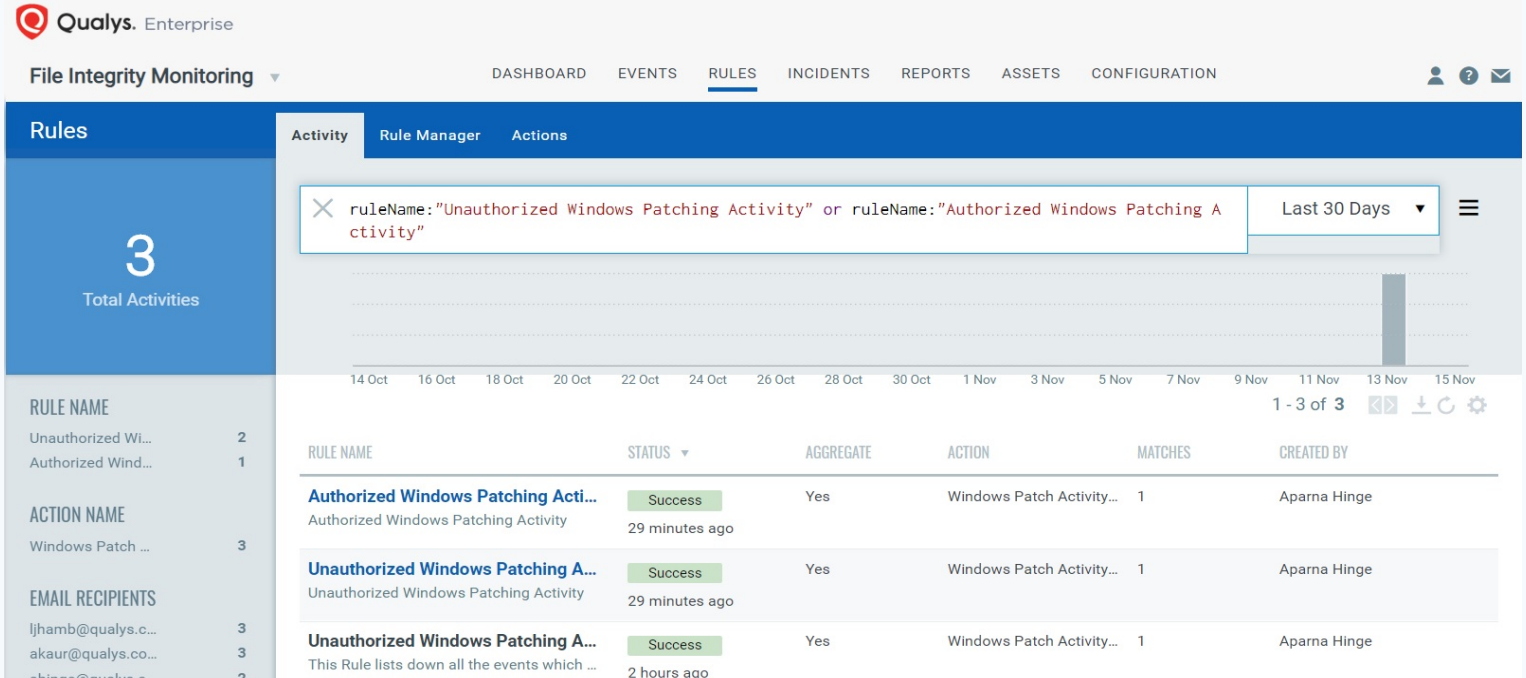
Qualys FIM: In just Second Year, 190+ customers

- Built on the same Qualys Cloud Agent you use for VM, PC
- Real-time detection for high volume, high scale
- Automated incident management and alerting
- Out of the box PCI monitoring profiles for OS and applications
- No infrastructure, data load for you to manage



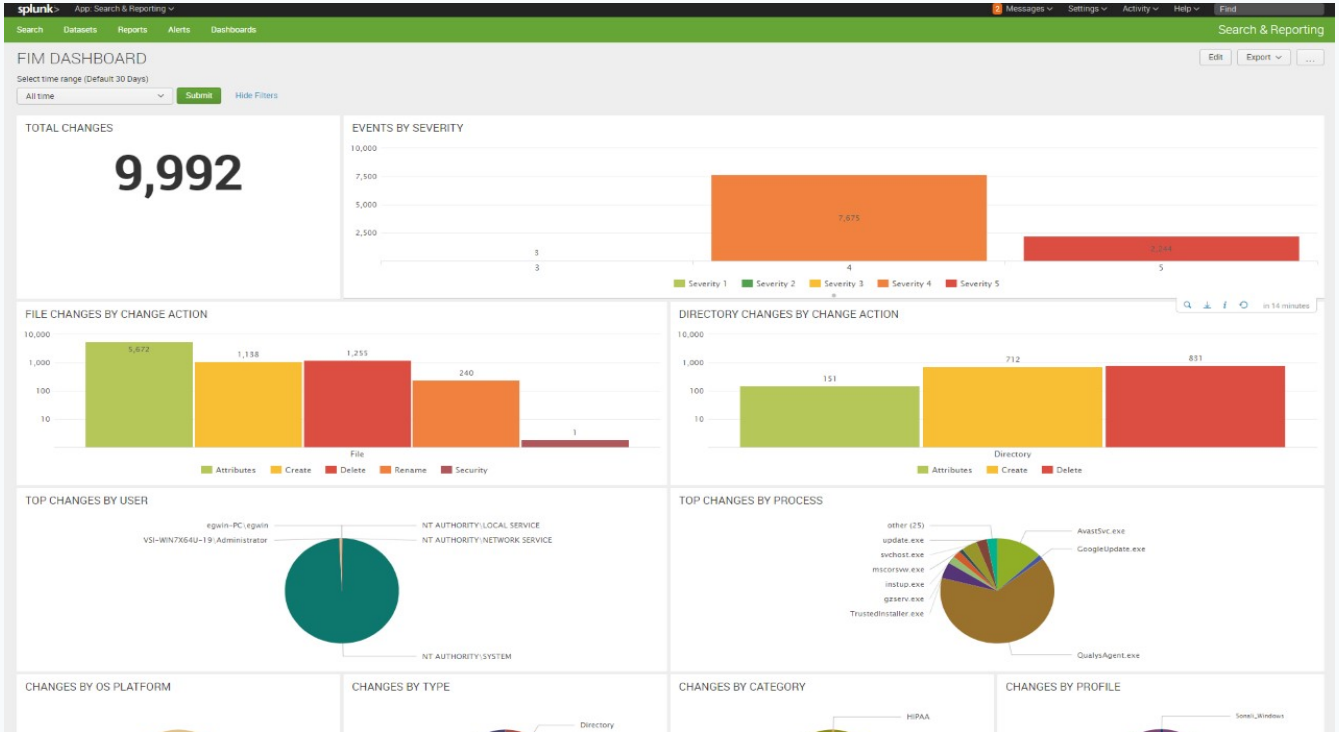
Qualys.

Alert and Incident Management for Authorized vs Unauthorized Changes During Patching with Qualys FIM

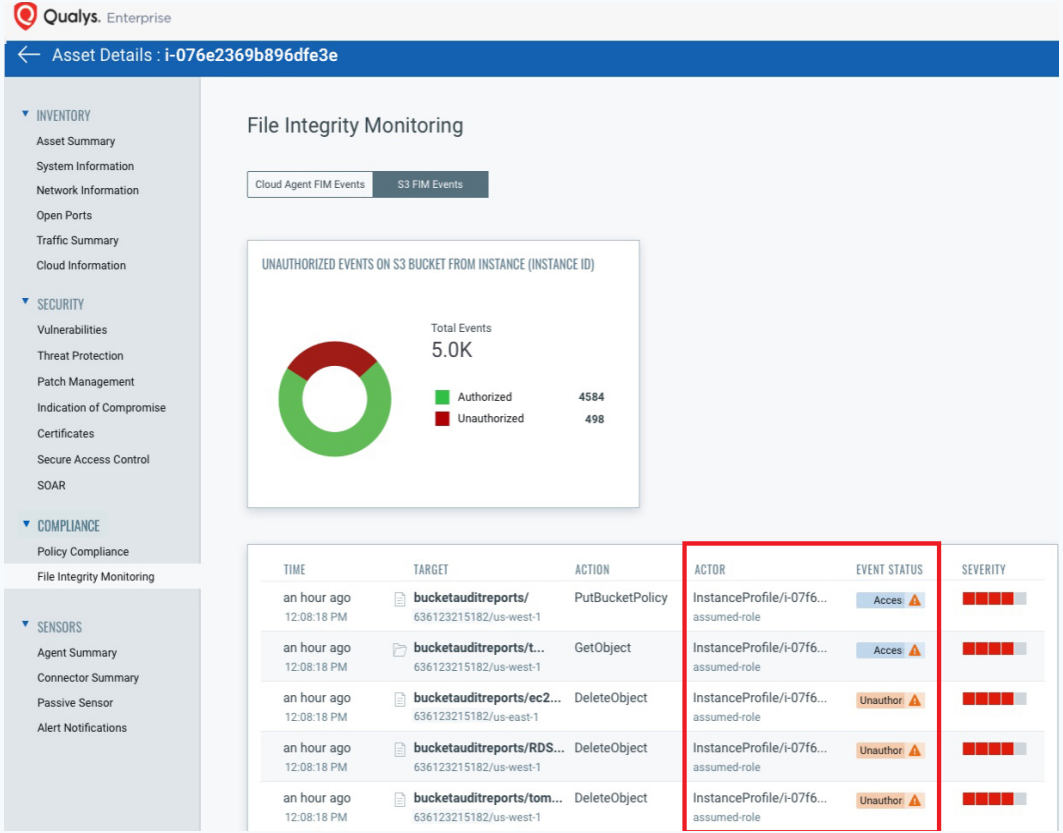


Qualys.

Open APIs: Integrate with Any External SIEM, DWH



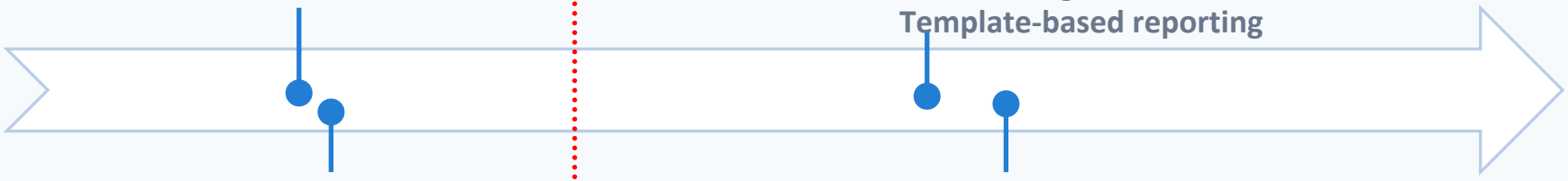
Qualys FIM gives context of changes in cloud



Qualys.

FIM Demo

FIM Roadmap



Q4 - 2019

Process, user and time-period inclusions and exclusions for event data collection

Q4 - 2019

FIM hosts health and status: % of hosts with latest data, stale hosts with no changes, hosts without a FIM monitoring profile

2020 Q1

Windows Registry monitoring for changes
Injection of PC FIM UDC data to FIM
FIM for cloud storage (S3 bucket content monitoring) – cloud-trail integration
Template-based reporting

2020 Q2

Monitoring for **file content changes/text changes**
External integration with JIRA, ServiceNOW
Monitoring profiles – import/exports
Patch Reconciliation: Integration with Qualys Patch Management for managing changes due to patching

Qualys.

Software as a Service (SaaS) Security & Compliance

Even Cloud is bloated; Need just SaaS Applications

Public cloud spending skyrockets as SaaS shines

IDG

IDC: Cloud spending to grow 21% by 2021

CIO DIVE

HR gets the cloud treatment

THE AUSTRALIAN

Workday Rises on Demand for Business Cloud-Based Software

Bloomberg

workday.

Namely

Office 365 box

Microsoft, Google Make Cloud Offerings More Enticing

eWEEK

Spending On CRM Apps Predicted To Soar In 2018

COMPUTERWORLD

salesforce

ZOHO

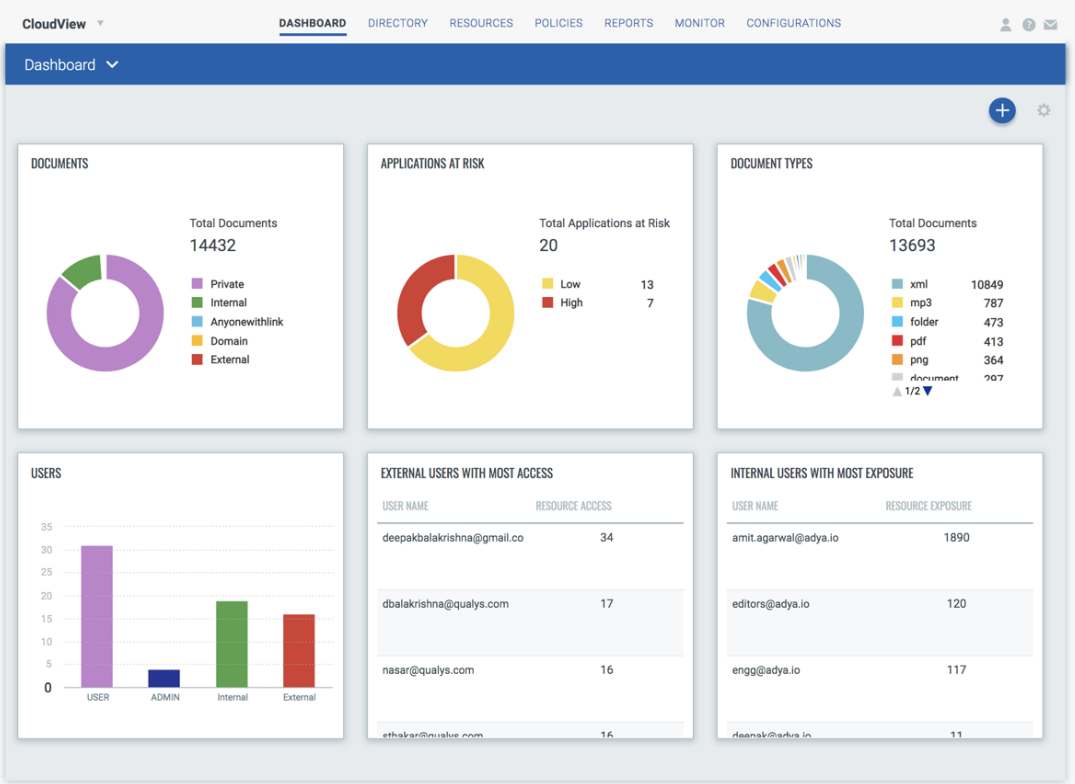
Qualys.

Manage Access, Exposure, Configuration and Compliance of SaaS Applications

Qualys SaaS Security and Compliance (SSC) enables

Inventory
Access
Exposure
Security Configurations

of SaaS applications and resources
E.g. Office365, Gsuite, Salesforce

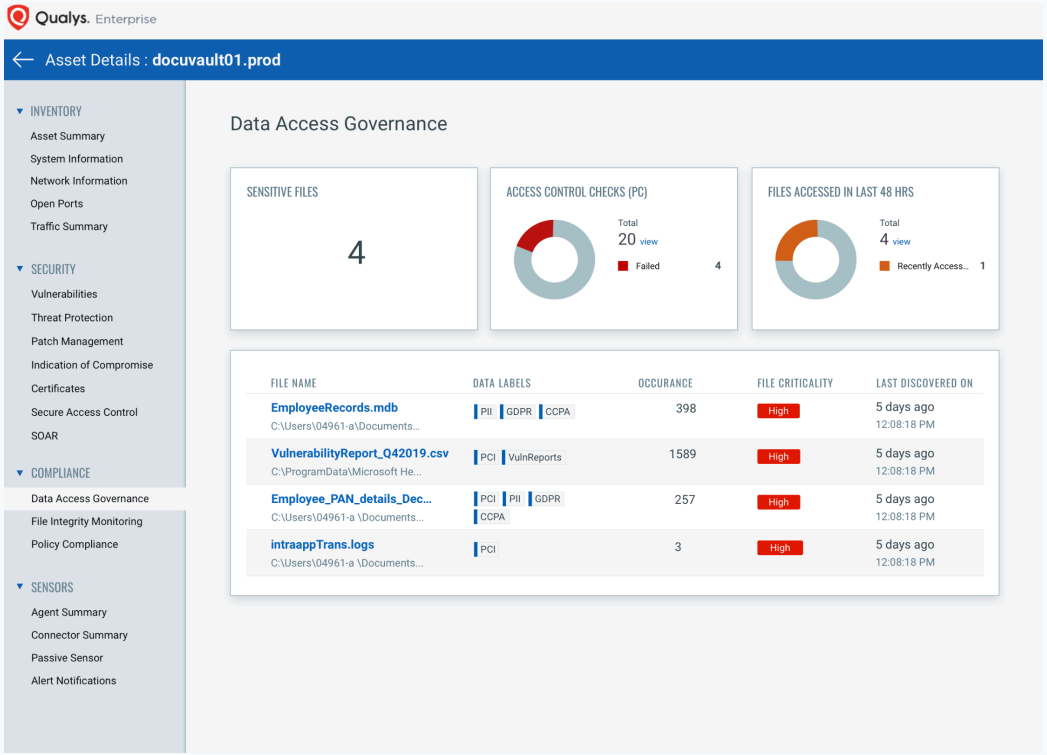


Discover Sensitive data and make sure it is secure and monitored for changes with Qualys DAG

Qualys Data Access Governance (DAG) will help with regulatory compliance

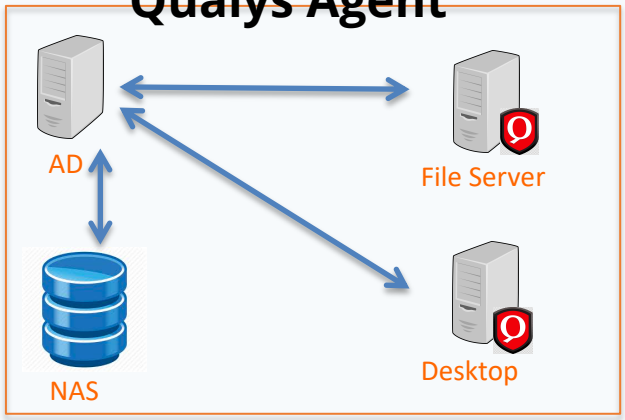
Discovery
Access Visibility
Activity Monitoring

For your sensitive, critical data



Cloud Applications

Qualys Agent



On Premise Unstructured Data

Directory / Metadata / access / classification

Adya/CV/CloudTrail

Directory / Metadata / access / based on rules

Qualys Cloud Platform

Unstructured Data Discovery

Visibility in ITAM – Know Assets hold sensitive data

Secure through PC - Create permission/share/access controls to check their access

Compliance

GDPR / CCA / HIPAA/ etc

Monitor them through FIM

Qualys.

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com